



User Guide

GD-RN-BP8616P

GD-RN-BP8632N

GD-RN-DT8864N

Contents

1 Introduction	5
1.1 Model Overview	5
2 Activate via Local Menu	6
3 Log In to Your Device	8
4 Network Settings.....	9
4.1 Network Parameter Settings.....	9
4.1.1 Configure TCP/IP	9
4.1.2 Configure DDNS.....	10
4.1.3 Configure PPPoE.....	11
4.1.4 Configure Multicast.....	11
4.2 Platform Access Settings	12
4.2.1 Configure SCMS.....	12
4.2.2 Configure ISUP	13
4.2.3 Configure SDK Service	14
4.2.4 Enable ISAPI.....	15
4.2.5 Configure ONVIF.....	15
4.2.6 Configure Log Server	16
4.3 Network Service Settings	16
4.3.1 Configure HTTP(S)	16
4.3.2 Configure RTSP.....	17
4.3.3 Configure WebSocket(s)	18
4.3.4 Configure Port Mapping (NAT)	18
5 User Management	21
6 Device Access	22
6.1 Access Video Device.....	22
6.1.1 Add Automatically Searched Online Network Camera.....	22
6.1.2 Add Network Camera Manually.....	23
6.1.3 Add Network Camera via Custom Protocol	24
6.1.4 Add Network Camera through Camera Configuration File.....	25

6.2 Add Access Control Device.....	25
6.3 Add Audio Device	25
6.4 Add POS Device	26
7 Camera Settings	28
7.1 Enable H.265 Stream Access	28
7.2 Batch Configuration	28
7.3 Display Settings	28
7.4 Configure Video Parameters.....	29
7.5 Configure Privacy Mask.....	30
8 Device Grouping.....	31
9 Storage Management	32
9.1 Manage HDD	32
9.2 RAID Configuration.....	33
9.2.1 Create Disk Array	33
9.2.2 Rebuild Array.....	35
9.2.3 Delete Array	35
9.2.4 View Firmware Info.....	36
9.3 Configure Storage Mode	36
9.4 Configure Other Storage Parameters	36
10 Schedule Configuration.....	38
10.1 Configure Schedule Template.....	38
10.2 Configure Recording Schedule	39
10.3 Configure Picture Capture Schedule.....	41
10.4 Configure Audio Recording	43
11 Live View	44
11.1 Configure Live View Layout.....	44
11.2 GUI Introduction	44
11.3 PTZ Control.....	45
12 Playback	47
12.1 GUI Introduction	47
12.2 Normal Playback	48

12.3 Event Playback	49
12.4 Sub-Period Playback.....	49
13 Event Center.....	51
13.1 Event Settings.....	51
13.1.1 Basic/Generic Event	51
13.1.2 Perimeter Protection	53
13.1.3 Abnormal Behavior Event	62
13.1.4 Target Event	65
13.1.5 Thermal Camera Detection	68
13.1.6 Alarm Input Event	69
13.1.7 Audio Analysis Event	71
13.2 Linkage Configuration	73
13.3 Event Search.....	74
13.4 View Alarms	75
14 Search and Backup	76
15 Smart Settings	78
15.1 Algorithm Management.....	78
15.2 List library Management	78
15.2.1 Add a List Library.....	78
15.2.2 Upload Face Pictures to the Library.....	78
16 Application Center	80
16.1 Human and Vehicle Detection	80
16.2 Person Check-In	80
16.2.1 Check-In Task	81
16.2.2 Search Check-In Records.....	81
16.3 Statistic Report.....	82
17 System Parameter Settings	83
18 Hot Spare Device Backup	84
18.1 Set Working Device	84
18.2 Set Hot Spare Device.....	84

19 Configure Exception Event	86
20 View System Info.....	87
21 System Maintenance.....	88
21.1 Schedule Reboot	88
21.2 Upgrade Device	88
21.3 Backup and Restore	88
21.4 Log Info.....	88
21.5 Configure Log Server	89
21.6 Maintenance Tools.....	89
22 Security Management.....	91
22.1 Address Filter	91
22.2 Stream Encryption.....	91
22.3 Select TLS Version	91
23 Appendix	92
23.1 List of Applicable Power Adapter.....	92
23.2 Glossary.....	93
23.3 Frequently Asked Questions	94
23.4 Notification for Corrosive Gas.....	96

1 Introduction

Thank you for purchasing a Grundig product. Before installing or connecting the product, please read first the following documents:

- Legal Disclaimer
- Safety Instructions
- Installation Manual and/or Quick Guide for the respective product model

Further information about the product like Data Sheets, CE Documents, etc. can also be found on our Webpage www.grundig-security.com.

This User Guide is a manual for Network Video Recorders. Please see in the list of 1.1 Model Overview the applicable models.

Please read this User Guide carefully and retain it for future use.

1.1 Model Overview

This User Guide is for the following products:

- GD-RN-BP8616P
- GD-RN-BP8632N
- GD-RN-DT8864N

2 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

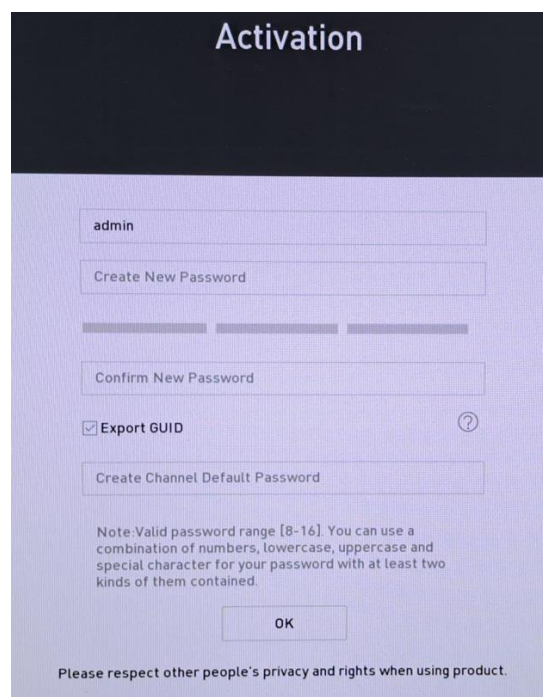
Ensure your device is connected with a monitor and mouse.

Steps

1. Power on your device.
2. Select a system language.
3. Enter the admin password twice.

Caution

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.



The screenshot shows the 'Activation' screen of a device. At the top, the word 'Activation' is displayed in white on a dark background. Below this, there are several input fields and a checkbox. The first field is labeled 'admin' and contains the text 'admin'. The second field is labeled 'Create New Password'. Below it is a progress indicator consisting of three horizontal bars. The third field is labeled 'Confirm New Password'. Below that is a checkbox labeled 'Export GUID' with a question mark icon to its right. The fourth field is labeled 'Create Channel Default Password'. Below the fields, there is a note: 'Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' At the bottom, there is an 'OK' button and a footer that reads 'Please respect other people's privacy and rights when using product.'

Figure 2-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.
5. Click **Activate**.

Note

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.
7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

3 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

1. Power on your device, you would automatically enter the login interface.

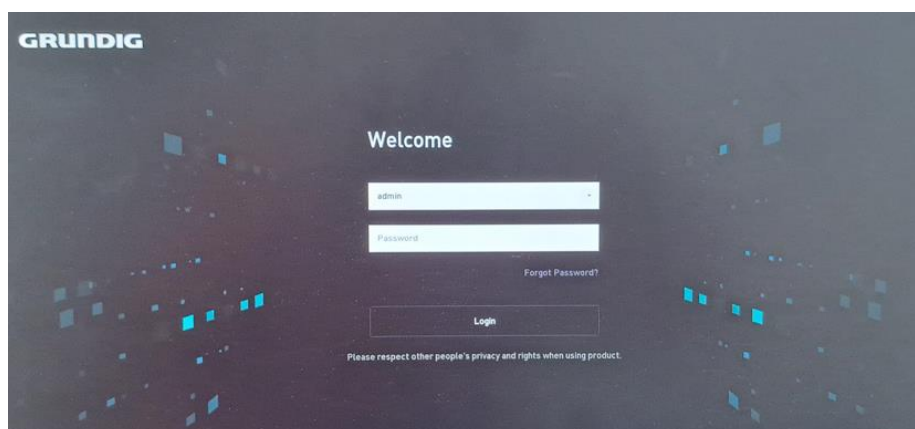


Figure 3-1 Login

2. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

Note

- Unlock pattern is only available for admin user.
 - If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.
-

4 Network Settings

Network parameters, platform access settings, and network services are configurable.

4.1 Network Parameter Settings

You shall configure network parameters before using functions that require network access.

4.1.1 Configure TCP/IP

TCP/IP must be properly configured before you operate video recorder over network or access network devices.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **TCP/IP**.

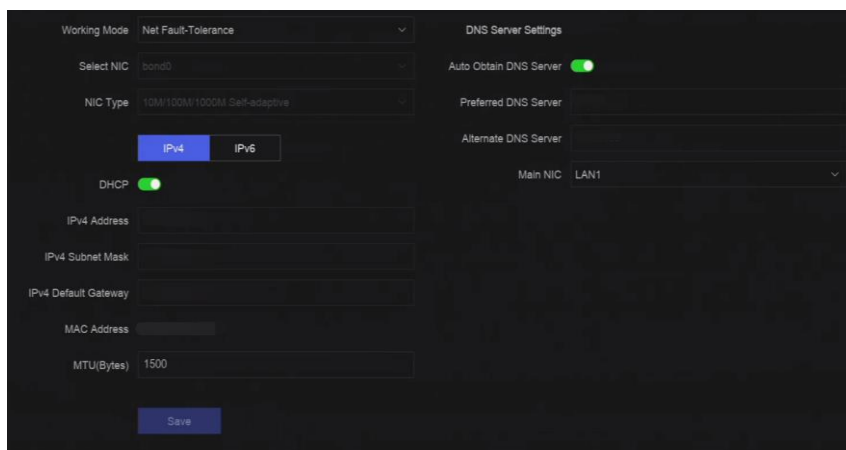


Figure 4-1 TCP/IP Settings

2. Set **Working Mode** and **Select NIC**.

Multi-address

The parameters of the two NIC cards can be configured independently. You can select **LAN1** or **LAN2** in the NIC type field for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet and the data will be forwarded through the default route.

Net-fault Tolerance

The two NIC cards use the same IP address, and you can set **Main NIC** to **LAN1** or **LAN2**. By this way, in case of one NIC card failure, the video recorder will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.

Note

Working mode is only available for certain models.

3. Configure network parameters.

IPv4**DHCP**

If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

MTU

The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

Auto Obtain DNS Server

If **DHCP** is enabled. You can check **Auto Obtain DNS Server** to obtain **Preferred DNS Server** and **Alternate DNS Server**.

IPv6**Router Advertisement**

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click **Save**.

4.1.2 Configure DDNS

Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **DDNS**.

Enable

DDNS Type: DynDNS

Server Address:

Device Domain Name:

User Name:

Password:

Status: DDNS is disabled.

Save

Figure 4-2 DDNS

2. Turn on **Enable**.
3. Select a DDNS type.
4. Set parameters, including service address, domain name, etc.
5. Click **Save**.

4.1.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPoE service.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **PPPoE**.

Enable

User Name:

Password:

Save

Figure 4-3 PPPoE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **Other**.
 2. Set **Multicast** parameters.
-

Note

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
 - For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.
-


3. Click **Save**.

4.2 Platform Access Settings

4.2.1 Configure SCMS

SCMS provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **System** → **System Settings** → **Network** → **SCMS**.
2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Click  to set verification code.
5. Optional: Enable **Stream Encryption**, **Sub-Stream Self-Adaptive Bitrate**, **Time Sync**, or edit server IP address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Sub-Stream Self-Adaptive Bitrate

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Time Sync

The device will sync time with SCMS instead of NTP server.

6. Download SCMS app. You can use a smart phone to scan the QR code to download SCMS app.
7. Use SCMS app to scan the device QR, and bind the device with your SCMS account.

Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

8. Click **Save**.

Result

- If your device is connected with SCMS, **Connection Status** will be **Online**.
- If your device is bound with a SCMS account, **Account Status** will be **Linked**.

What to do next

You can access your video recorder via SCMS.

4.2.2 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System** → **CX** → **System Settings** → **Network** → **Platform Access** → **ISUP**.

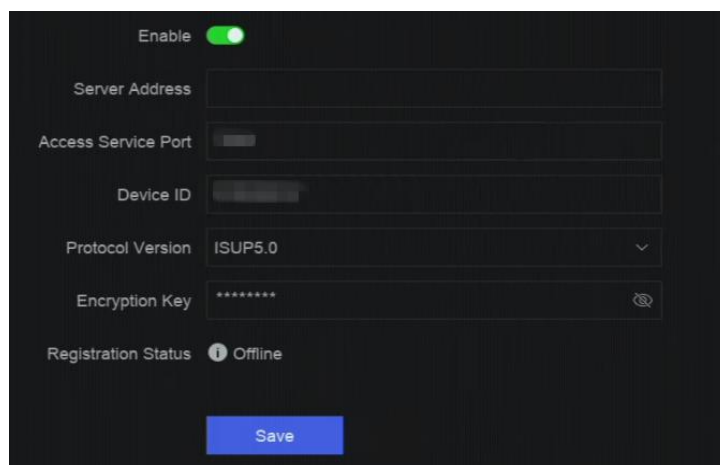


Figure 4-5 ISUP

2. Turn on **Enable**.

Note

If ISUP is enabled, the SCMS access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click **Save**.

You can see the registration status (online or offline) after the device is restarted.

4.2.3 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to **System** → **System Settings** → **Network** → **Platform Access** → **SDK**.

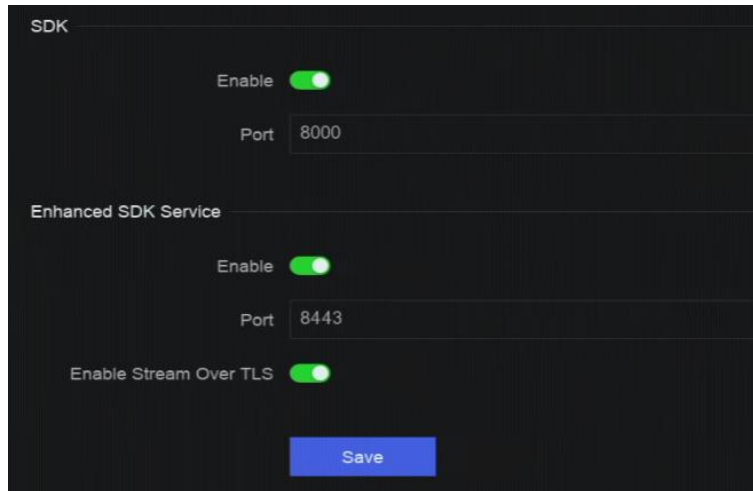


Figure 4-6 SDK Service

2. Configure **SDK** and **Enhanced SDK Service** according to your requirement.

Note

The port for **Enhanced SDK Service** is 8443 by default.

- Optional: Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- Click **Save**.

4.2.4 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to **System** → **System Settings** → **Network** → **Platform Access** → **ISAPI** to enable the function.

4.2.5 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

- Go to **System** → **CX** → **System Settings** → **Network** → **Platform Access** → **ONVIF**.

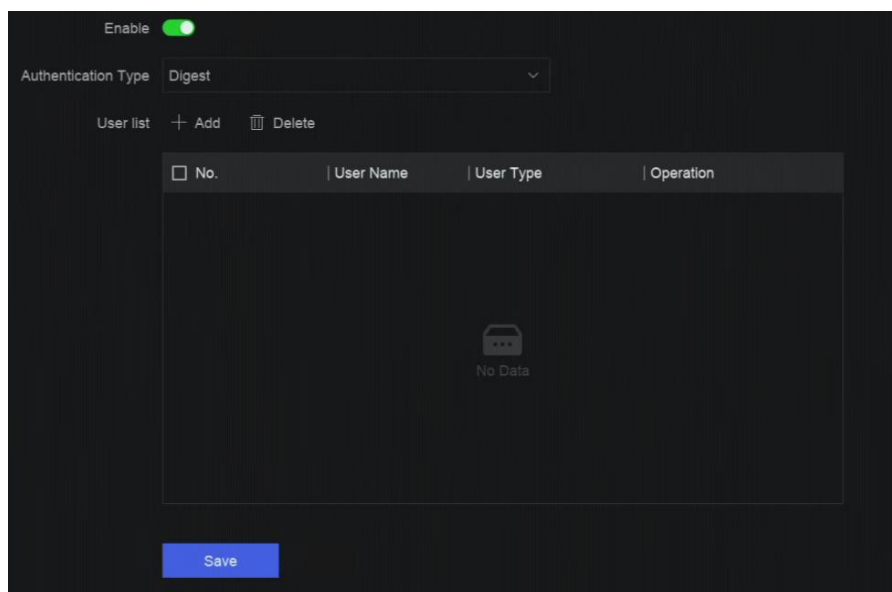


Figure 4-7 ONVIF

- Turn on **Enable**.
- Select an authentication type.
- Click **Add** to add a user.
- Set the user name and password.

Caution

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product

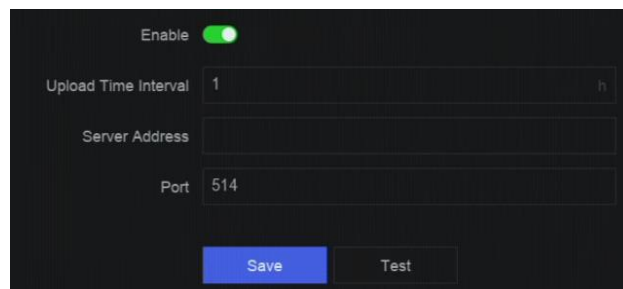
6. Click **Save**.

4.2.6 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to **System** → **System Settings** → **Network** → **Platform Access** → **Log Server**.



The screenshot shows a configuration panel for the Log Server. At the top, there is an 'Enable' toggle switch that is turned on (green). Below it, there are three input fields: 'Upload Time Interval' with a value of '1' and a unit of 'h', 'Server Address' which is currently empty, and 'Port' with a value of '514'. At the bottom of the panel, there are two buttons: 'Save' and 'Test'.

Figure 4-8 Log Server

2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. Optional: Click **Test** to check if parameters are valid.
5. Click **Save**.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **HTTP(S)**.

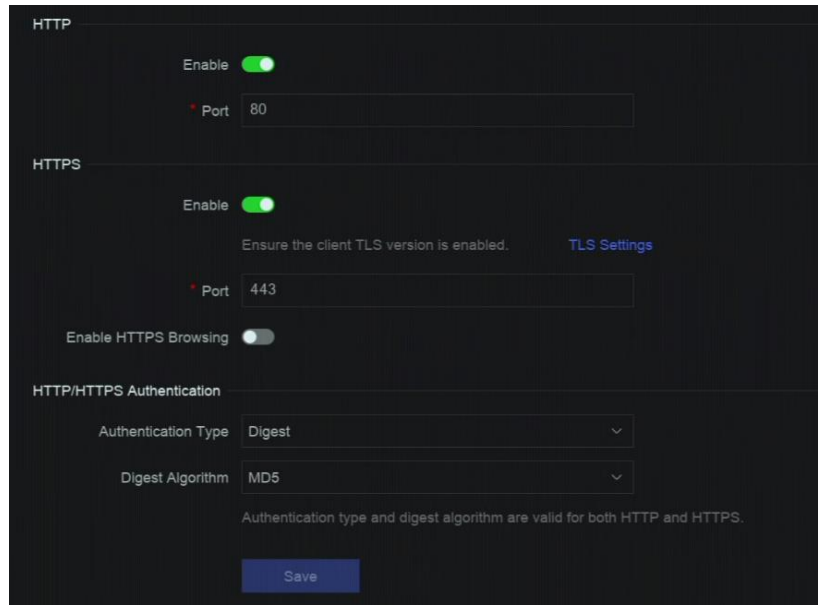


Figure 4-9 HTTP(S)

2. Optional: Turn on HTTP or HTTPS.
3. View or edit **Port** of HTTP or HTTPS.
4. Set **HTTP/HTTPS Authentication**.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click **Save**.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **RTSP**.

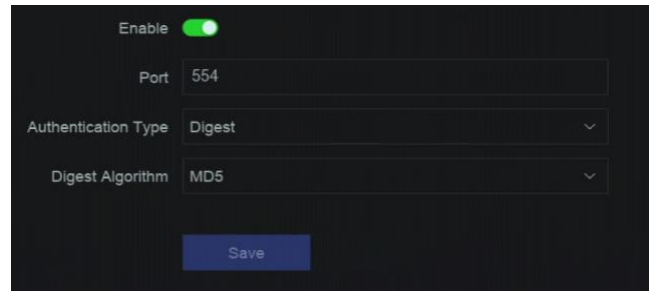


Figure 4-10 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

Two authentication types are selectable, if you select **Digest**, only the request with digest authentication can access the video stream by RTSP via the IP address. For security reasons, it is recommended to select **Digest** as the authentication type.

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click **Save**.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **WebSocket(s)**.
2. Turn on **Enable**.
3. Set **Port**.
4. Click **Save**.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ (Universal Plug and Play), and manual mapping. UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **NAT**.

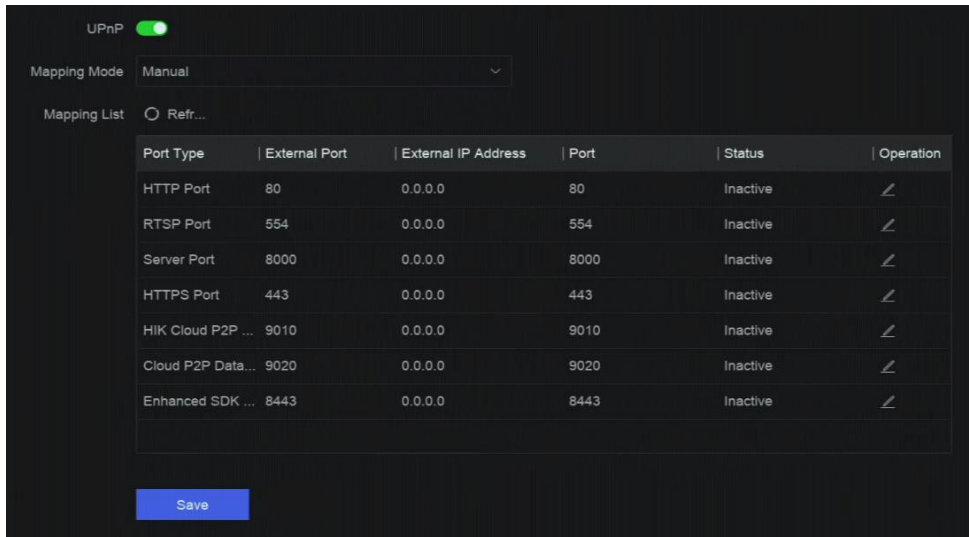


Figure 4-11 Port Mapping (NAT)


2. Turn on **Enable**.
3. Set **Mapping Mode**.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If **Mapping Mode** is selected as **Manual**, click  to edit corresponding ports.

Note

- The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.
- **External Port** indicates the internal port number for port mapping in the router.

5. Click **Save**.

What to do next

Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.

5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to **System** → **System Settings** → **User Management**.

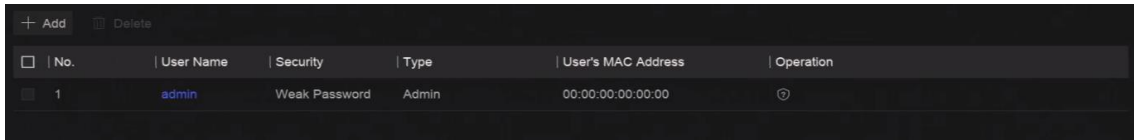


Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
	Set account security.
Add	Add a new guest or operator user.
	Delete the selected user.

Note

Before operation, you have to confirm the admin password.

6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device** → **Online Device List**.
2. Select the device(s) from the list.

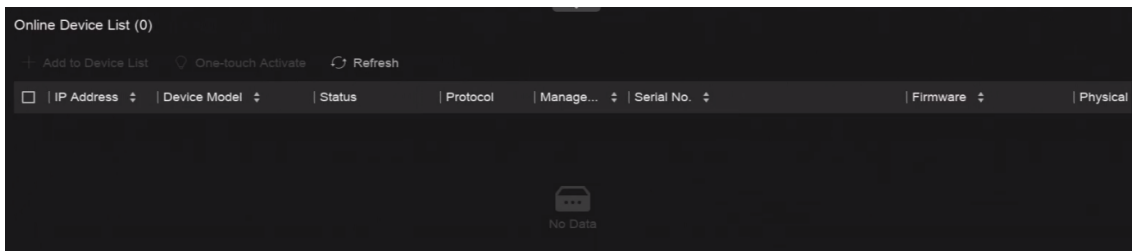


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click **Add to Device List**.

Note

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.

Ensure the network camera is activated.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.

The screenshot shows a web interface titled "Add Device". At the top, there is a section for "Online Device List (0)" with a "Refresh" button. Below this is a table with columns: "No.", "IP Address", "Device Model", "Status", "Protocol", "Manag...", and "Serial No". The table is currently empty, showing "No Data". Below the table are several input fields: "IP Address" with a "Test" button, "Device Name" (filled with "IPCamera 01"), "Protocol" (a dropdown menu showing "ONVIF"), "Management Port" (filled with "80"), "User Name" (filled with "admin"), "Password", and "Transfer Protocol" (a dropdown menu showing "Auto"). There is also a checkbox labeled "Use Channel Default Password".

Figure 6-2 Add Network Camera Manually

2. Click **Add**.
3. Enter network camera parameters.

Use Channel Default Password

If it is enabled, the video recorder will add the camera by the set channel default password.

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

4. Optional: Click **Continue to Add** to add other network cameras.
5. Click **Add**.

6.1.3 Add Network Camera via Custom Protocol

For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.
2. Click **More** → **Custom Protocol Management**, or **Add** → **Protocol Management**.

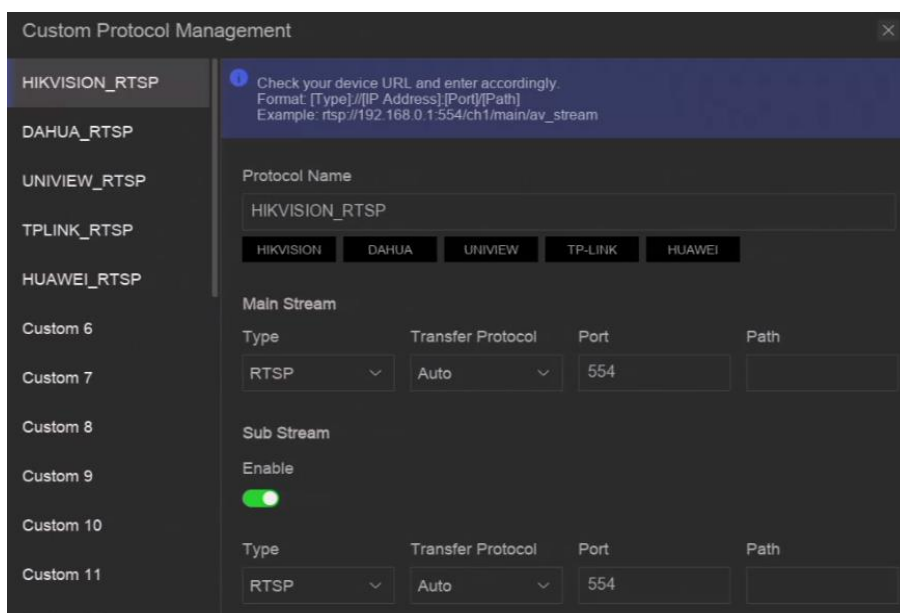


Figure 6-3 Add Network Camera via Customized Protocol

3. Select a protocol type at the left side.
4. Set protocol parameters.

Type

The network camera adopting custom protocol must support getting stream through standard RTSP.

Transfer Protocol

3 types are selectable, including **Auto**, **UDP**, and **RTP Over RTSP**.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and sub-stream. The general format is *[Type]://[IP Address]:[Port]/[Resource Path]*, for example, *rtsp://192.168.0.1:554/ch1/main/av_stream*.

Note

- **Protocol Name** and **Path** can be automatically generated if you click a brand name below **Protocol Name**.

You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.

5. Click **OK**.

6. Click **Add** in **System** → **Device Access** → **Device** → **Video Device** to manually add a network camera.

6.1.4 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.
2. Click **Import** to import the configuration file in USB flash drive.
3. Set the folder path.
4. Click **Confirm**.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.
The adding process is similar with **Access Video Device**.

6.3 Add Audio Device

Audio devices can be added to your video recorder.
The adding process is similar with **Access Video Device**.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

1. Go to **System** → **Device Access** → **Device** → **POS**.
2. Click **Add** to add a POS device.

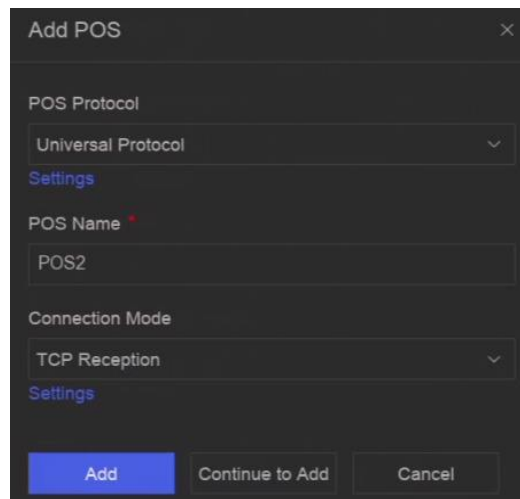


Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click **Add**.

Note

After a POS device is add, you can click  in **Operation** to configure POS text overlay.

7 Camera Settings

You can configure the added camera, such as privacy mask, image parameters, etc.

7.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.
2. Click **More** → **Auto Switch to H.265**.
3. Enable this function.
4. Click **Save**.

7.2 Batch Configuration

Cameras can be configured in a batch.

Steps

1. Go to **System** → **Device Access** → **Device Configuration** → **Batch Configuration**.

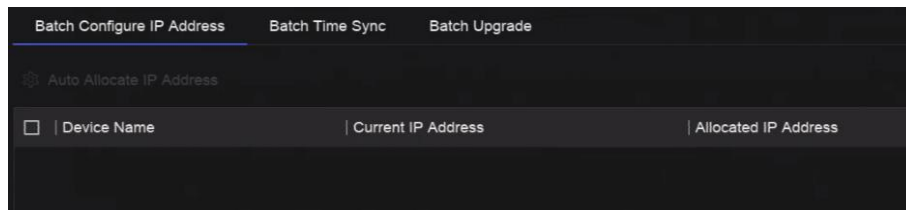


Figure 7-1 Batch Configuration

2. Configure IP address, sync time, or upgrade firmware as your desire.
3. For IP address configuration and time sync, click **Save**.

7.3 Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Go to **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Display Settings**.

Select a camera, and configure parameters as your desire.

OSD Settings

Configure the OSD (On-screen Display) settings for the camera, including date/time, camera name, etc.

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.

Image Enhancement

For optimized image contrast enhancement.

7.4 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Video Parameters**. Select a camera, and configure parameters as your desire.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

It refers to the number of frames captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

7.5 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Privacy Mask**.

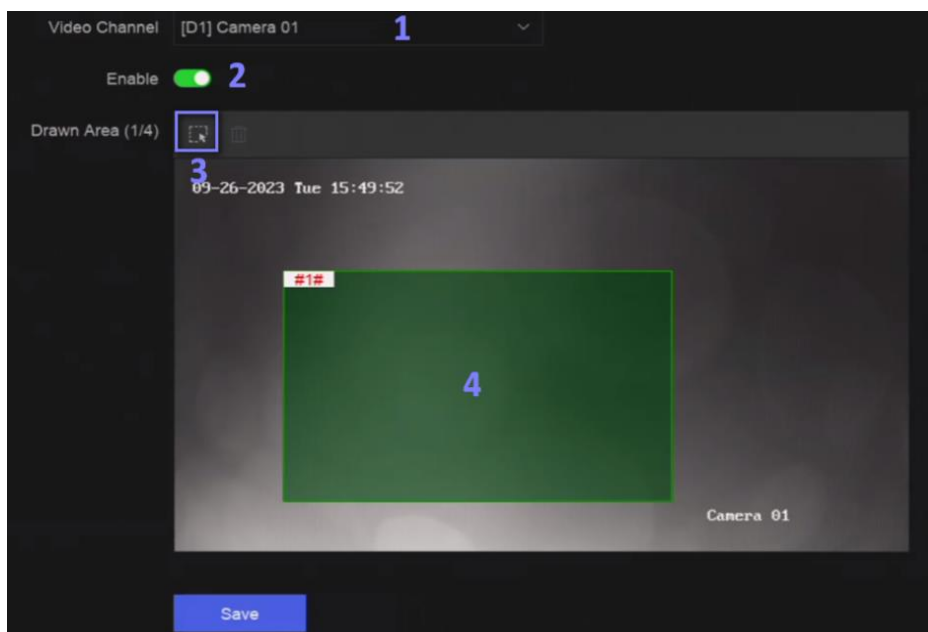


Figure 7-2 Privacy Mask

2. Select a camera.
3. Turn on **Enable**.
4. Draw mask areas on the preview window. The areas will be marked with different frame colors.

Note

Up to 4 privacy mask areas can be configured and the size of each area can be adjusted.

5. Click **Save**.

8 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to **System** → **Device Access** → **Device Grouping**.

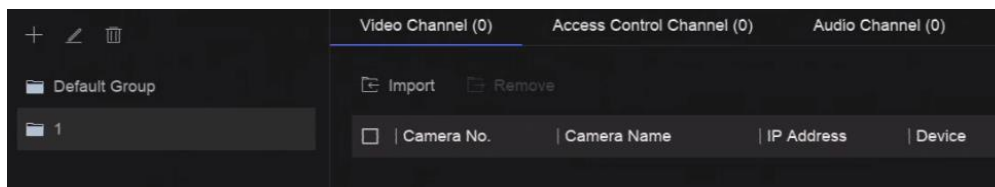


Figure 8-1 Device Grouping

2. Click **+** to add a group.

Note

After a group is added, you can click **✎/🗑** to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

9 Storage Management

9.1 Manage HDD

A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start

Ensure the HDD is properly installed to your device.

Steps

1. Go to **System** → **Storage Management** → **Storage HDD** → **Storage HDD**.

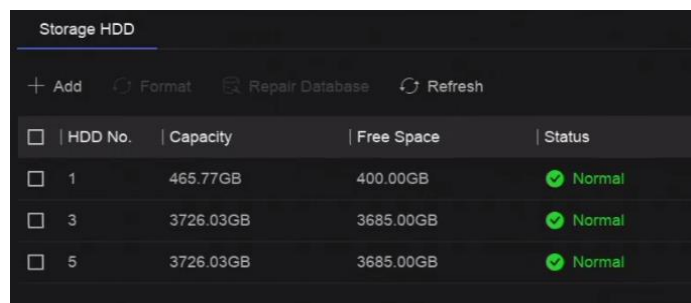


Figure 9-1 Manage HDD

2. Optional: Perform the following operations as your desire.

Add Add a network HDD.

Format Format the selected HDD.

Repair Database Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
 - Do not pull out the drive, or shut down the device during the process.
-



Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

Caution

RAID requires enterprise-level HDDs.

The functions in this section is only available for GD-RN-DT8864N. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

Table 9-1 HDD Requirement for Each RAID Type

RAID Type	Required Number of HDDs
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Note

- The function is only available for certain models.
 - When array exception event occurs, the corresponding linkage actions can be configured in **System → System Settings → Exception**.
-

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- **Storage Mode** is set to **Quota** in **System → Storage Management → Storage Mode**.
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management**.
2. Click **Enable Array Mode**, or enable **Array Mode**.

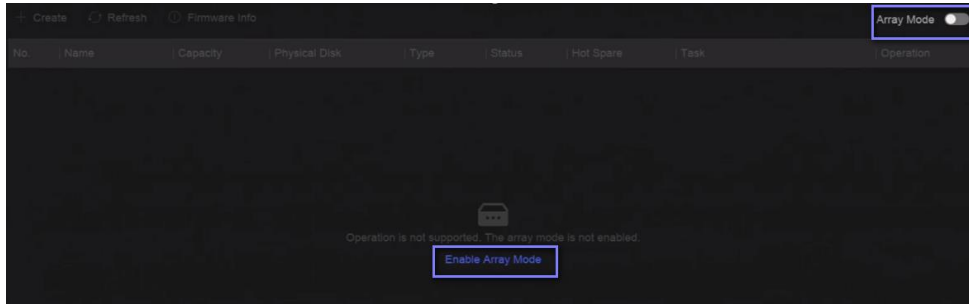


Figure 9-2 Enable RAID

3. Wait for the device to restart.
4. Go to **System** → **Storage Management** → **Storage HDD** → **Array Management** again.

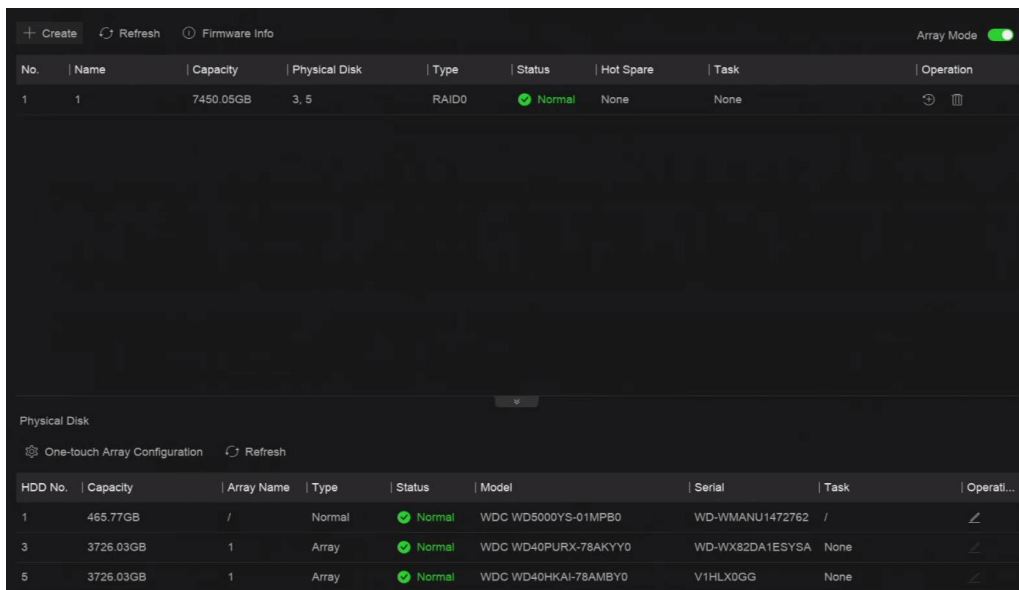


Figure 9-3 Array Management

5. Create an array.

Creation Method

Description

One-touch Array Configuration

Click **One-touch Array Configuration**.

Note

By default, the array type created by one-touch configuration is RAID 5.

Manual Creation

Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.


9.2.2 Rebuild Array

The array status includes **Functional**, **Degraded**, and **Offline**. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Steps

1. Go to **System** → **Storage Management** → **Storage HDD** → **Array Management**.
2. Rebuild an array.

Table 9-2 Rebuilding Method

Rebuilding Method	Description
Auto Rebuild	<p>There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click  in Operation column under Physical Disk to set a hot spare disk.</p> <p>When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.</p> <hr/> <p>Note</p> <p>After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.</p> <hr/>
Manual Rebuild	<p>If there is no hot spare disks in the array, you have to manually rebuild the array.</p> <p>Go to System → Storage Management → Storage HDD → Array Management, and select the hot spare disk in the list to rebuild.</p>

9.2.3 Delete Array

Go to **System** → **Storage Management** → **Storage HDD** to click  to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

1. Go to **System** → **Storage Management** → **Storage HDD** → **Array Management**.
2. Click **Firmware Info**.
3. Optional: Set **Back Ground Task Speed**.

9.3 Configure Storage Mode

Steps

1. Go to **System** → **Storage Management** → **Storage Mode**.

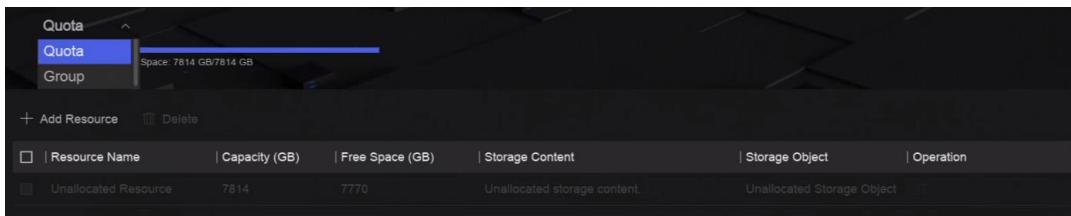


Figure 9-4 Storage Mode

2. Select **Quota** or **Group**.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group



Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.

3. Set corresponding parameters.
 - **Quota:** Allocate space for storage objects.
 - **Group:** Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to **System** → **Storage Management** → **Advanced Settings**.

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	When the HDD is not used for a period, it will turn to sleep.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Time for Clip Export	When videos are exported from the device, package time means the video duration of each video package file.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.
Tag Video Post-Record	<p>After adding a tag to a video, it is the time you set to record after the scheduled time.</p> <hr/> <p>Note</p> <ul style="list-style-type: none"> ● You can click  during live view or playback to add a tag. ● For searching tag videos, go to  → Backup → By Tag. <hr/>

10 Schedule Configuration

The device will follow the schedule to store files to the disk.

10.1 Configure Schedule Template

After a schedule template is configured, you can use the template as the recording schedule.

Steps

1. Go to **System** → **System Settings** → **Template Configuration** → **Holiday Schedule**.
2. Click **Add**.

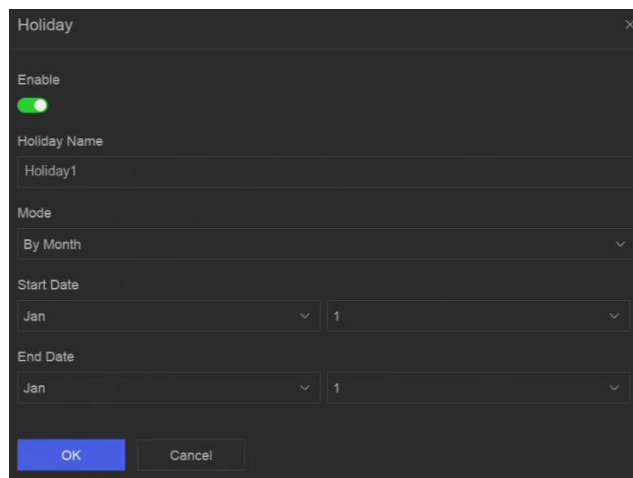


Figure 10-1 Add Holiday

3. Turn on **Enable**.
4. Configure the holiday.

Note

After holidays are configured, you will be able to set the holiday schedule independently. Holiday schedule has higher priority than normal schedule (from Mon to Sun).

5. Set **Storage Schedule**.
 - 1) Click **Storage Schedule**.
 - 2) Select a template name.

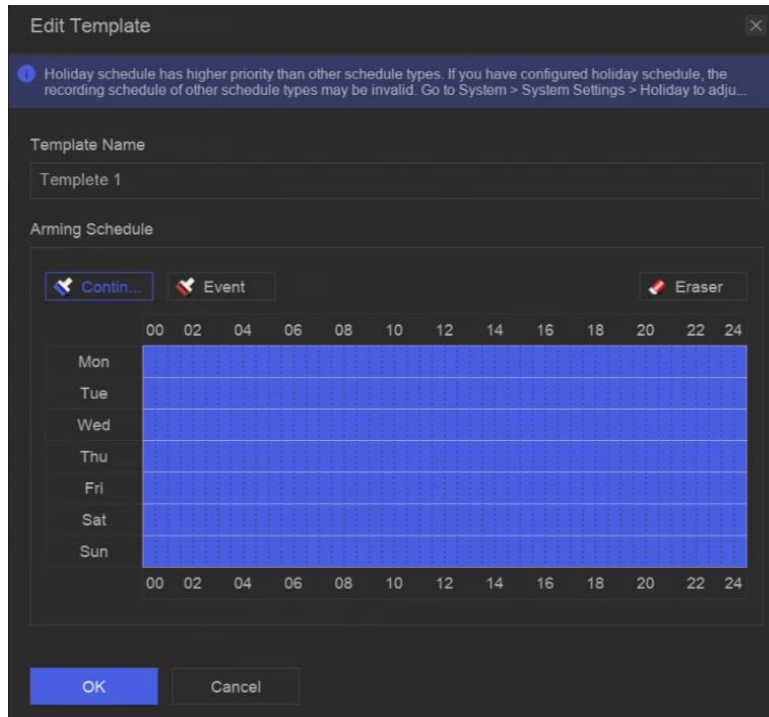



Figure 10-2 Edit Template

- 3) Select a recording type. For example, **Event**.
- 4) Drag the cursor on time bar to draw the schedule.

Note

- After moving the cursor on time bar, you can also click **00:00-24:00**  to set specified time schedule.
 - You can click **Eraser** to clear schedule.
-

Note

You can also click **Configure Template** to configure template in **System** → **Storage Management** → **Storage Schedule** → **Video Recording / Picture Capture / Audio Recording**.

6. Click **OK**.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to **System** → **Storage Management** → **Storage Schedule** → **Video Recording**.

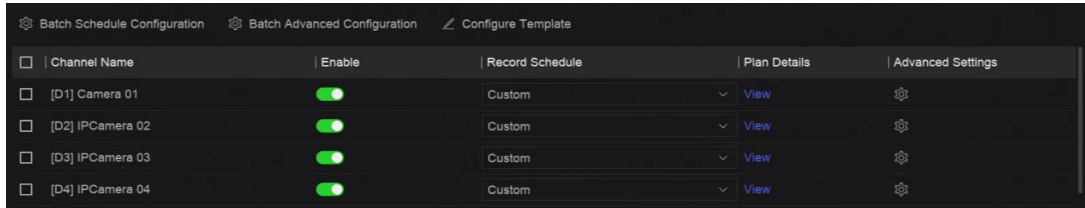


Figure 10-3 Video Recording Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.

Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

4. Click **View** to view the schedule.



Figure 10-4 View Schedule

5. Optional: Click  under **Advanced Settings** to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.

Parameter	Description
	<hr/> <p>Note</p> <p>The channel shall have audio function, or have connected an audio device.</p> <hr/>
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

6. Optional: Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

1. Go to **System** → **Storage Management** → **Storage Schedule** → **Picture Capture**.

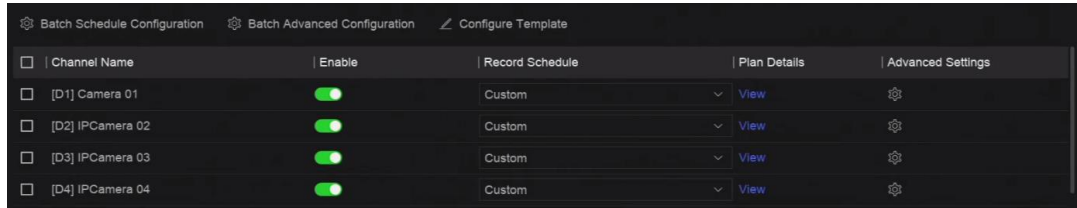


Figure 10-5 Picture Capture Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.

Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

4. Click **View** to view the schedule.



Figure 10-6 View Schedule

5. Click under **Advanced Settings** to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.

Parameter	Description
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

- Optional: Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
- Click **Save**.


10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

- Go to **System** → **Storage Management** → **Storage Schedule** → **Audio Recording**.
- Turn on **Enable** for a channel.
- Select a schedule type.

Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

- Click **View** to view the schedule.
- Optional: Click under **Advanced Settings** to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.




- Optional: Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
- Click **Save**.

11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

1. Go to **Live View**.
2. Click  at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click .
6. Set the live view image output interface. You can drag a channel from the channel list to a window, or drag a channel from one window to another.
7. Click .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.

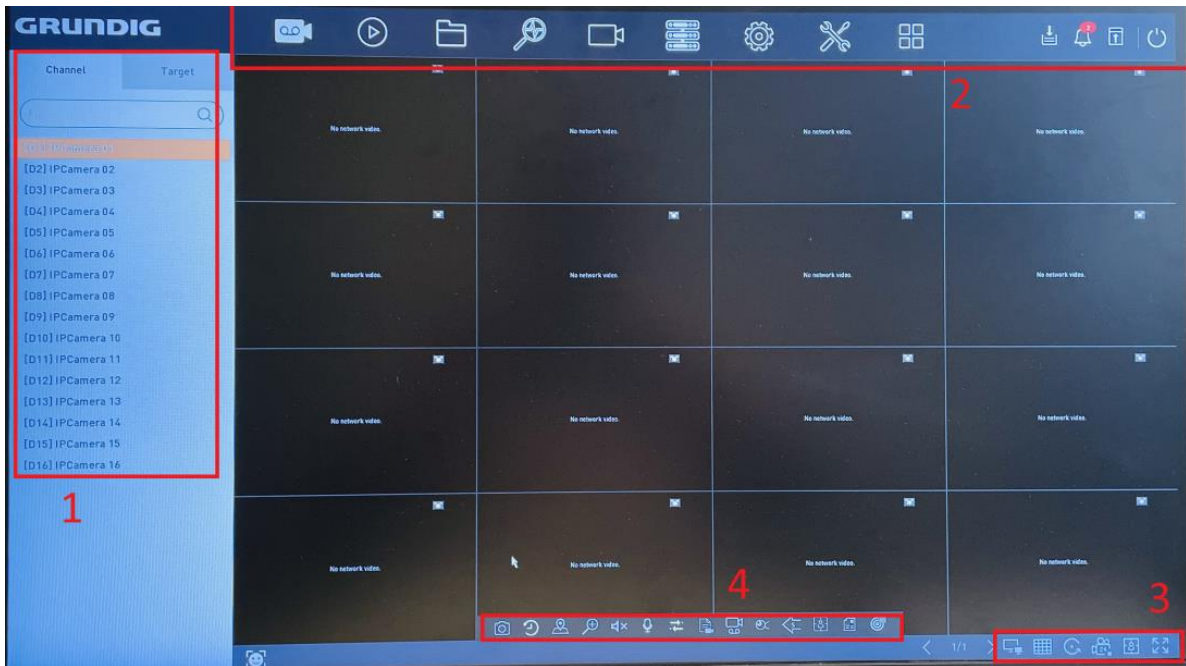





Figure 11-1 Live View





Table 11-1 Interface Description



No.	Description
1	Channel list, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Shortcut menu. It will appear after clicking the cursor on the image area.
3	Channel tool bar. <ul style="list-style-type: none"> • Click  to add a tag go the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. • You can select  → Show VCA Info to display rule frames.
4	Live view tool bar.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out. Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Table 11-2 PTZ Operation

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	Set a preset: <ol style="list-style-type: none"> 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click .
		Call a preset: Click  .
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are corresponded to the presets.	Set a patrol: <ol style="list-style-type: none"> 1. Select a patrol. 2. Click . 3. Add presets for the patrol. 4. Click OK.
		Call a patrol: Click  .

Task	Description	Operation
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: 1. Click  . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording.
		Call a pattern: Click  .

Note

If the PTZ panel cannot be used, please click  to check the settings.

12 Playback

12.1 GUI Introduction

You can play back video or audio files.

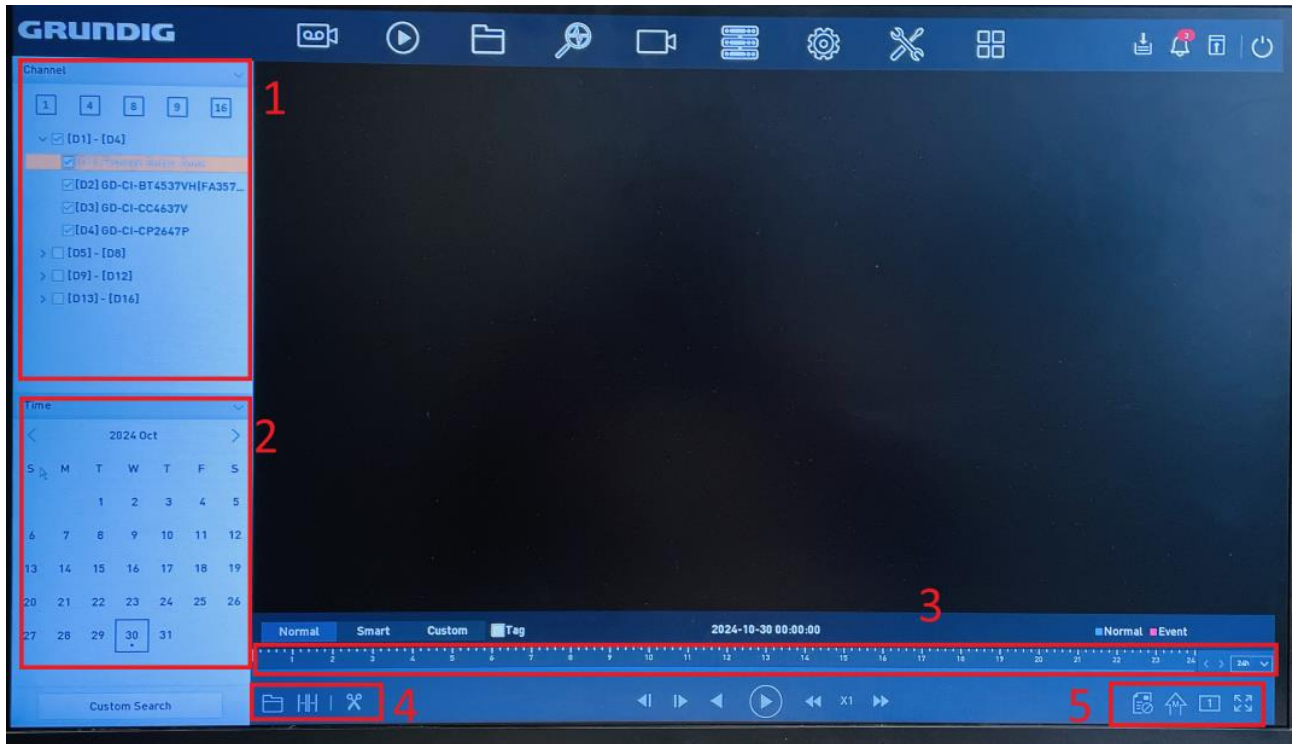








Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Channel list.
2	Calendar for time selection.
3	Playback timeline. <ul style="list-style-type: none"> ● Position the cursor on the timeline, drag the timeline to position to a certain time. ● Period marked with blue bar contains video. Red bar indicates the video in the period is event video. ● Scroll up/down to zoom out/in timeline.
4	Channel tool bar. <ul style="list-style-type: none"> ● Click  to add a tag go the channel. After adding, you can go to  → Backup → By Tag to search

No.	Description
	<p>videos by tag.</p> <ul style="list-style-type: none"> Click  to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to  → Backup → By Tag to search videos by lock. Select  → Dual-VCA to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type. <hr/> <p>Note</p> <p>In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface.</p> <hr/> <ul style="list-style-type: none"> You can select  → Show VCA Info to display rule frames.
5	<ul style="list-style-type: none"> Playback strategy

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

1. Go to **Playback**.
2. Select channel(s) in the list on the top.


Note

Group playback: Select a group in the list, and channels in the group can be played back.

3. Select a date in the calendar.

Note

The blue triangle at the calendar date corner indicates there are available videos.

4. Optional: Play back videos that contain human or vehicle targets.
 - : Videos that contain human would be marked in red.

- : Videos that contain vehicle would be marked in red.


12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start



- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration** → **Video/Audio** → **Display Info. on Stream**.
- Ensure your video recorder has enabled **Save Camera VCA Data** in **Storage management** → **Advanced Settings**.

Steps

1. Select **Playback** → .
2. Select a date in the calendar.

Note

The blue triangle at the calendar date corner indicates there are available videos.

3. Click  → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
4. Click **Search**.
Videos meet the detection rule requirement will be marked in red.
5. Click  to set normal video and smart video (the video that contains smart data) playback strategy.

Note

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Sub-Period Playback

The video files can be played in multiple sub-periods simultaneously on the screen.

Steps

1. Go to **Playback**.
2. Select a camera.
3. Set the start time and end time.
4. Click **Search**.

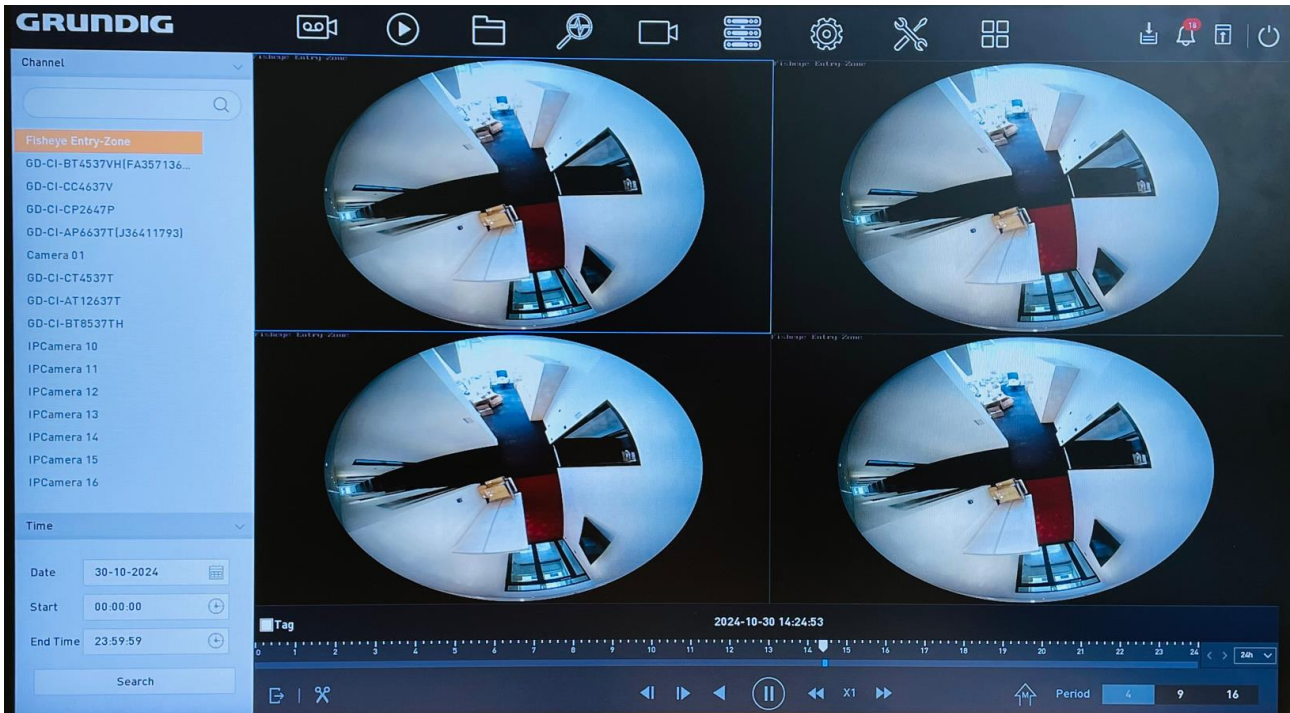


Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

Note

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps


1. Go to **Event Center** →  → **Event Configuration** → **Basic Event / Generic Event**.
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

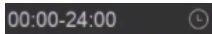
Table 13-1 Normal Event

Event Name	Event Description	Rule Configuration	
Motion Detection	Motion detection detects the moving objects in the monitored area.	<p>Use the tool bar at the top of image to draw the detection area.</p> <p>AI by NVR</p> <p>The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.</p> <p>AI by Camera</p> <p>The motion detection event will be analyzed by camera.</p> <p>Detection Target</p>	<p>Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.</p>

		Human and Vehicle are selectable, apart from false alarms, only the selected target(s) can trigger alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-2 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

8. Click **Save**.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Before You Start

Please go to **System** → **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection** to enable **Perimeter Protection** algorithm.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. Optional: Turn on **Enable AI by NVR**.
The device will analyze the video, and cameras only transmit video stream.
4. Select **Line Crossing**.
5. Turn on **Enable**.

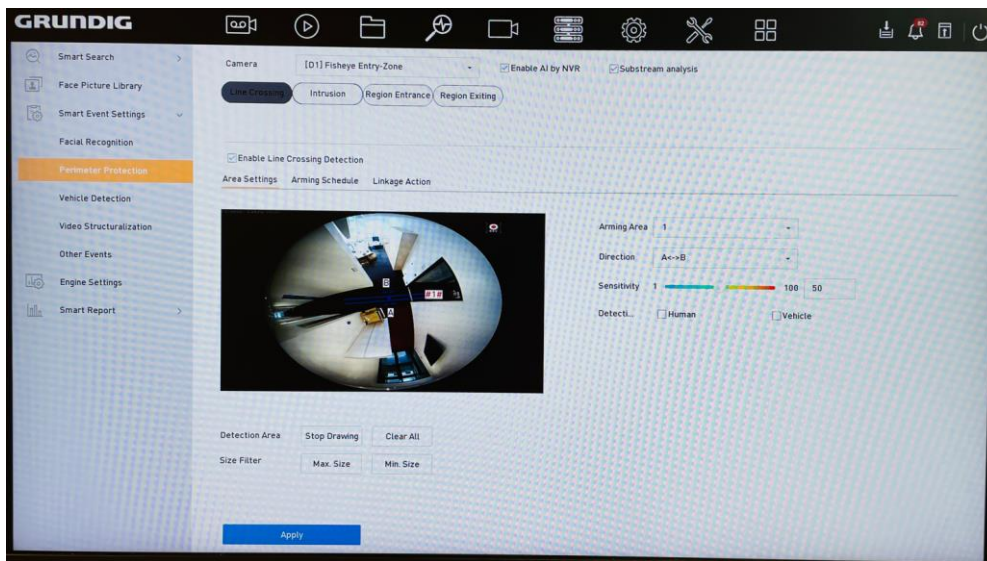



Figure 13-1 Line Crossing Detection

6. Click **Rule Settings** to detection rules.
 - 1) Select a rule number. For example, select **1**.
 - 2) Click , and click on the image twice respectively to draw the start point and end point of the detection line.
 - 3) Set **Direction**, **Sensitivity**, and **Detection Target**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A



Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

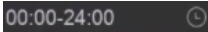
The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) Optional: Click /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) Optional: Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

- 8. Click **Linkage Method** to set linkage methods.

Table 13-3 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.
10. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a pre-defined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

Please go to **System** → **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection** to enable **Perimeter Protection** algorithm.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. Optional: Turn on **Enable AI by NVR**.
The device will analyze the video, and cameras only transmit video stream.
4. Select **Intrusion**.
5. Turn on **Enable**.

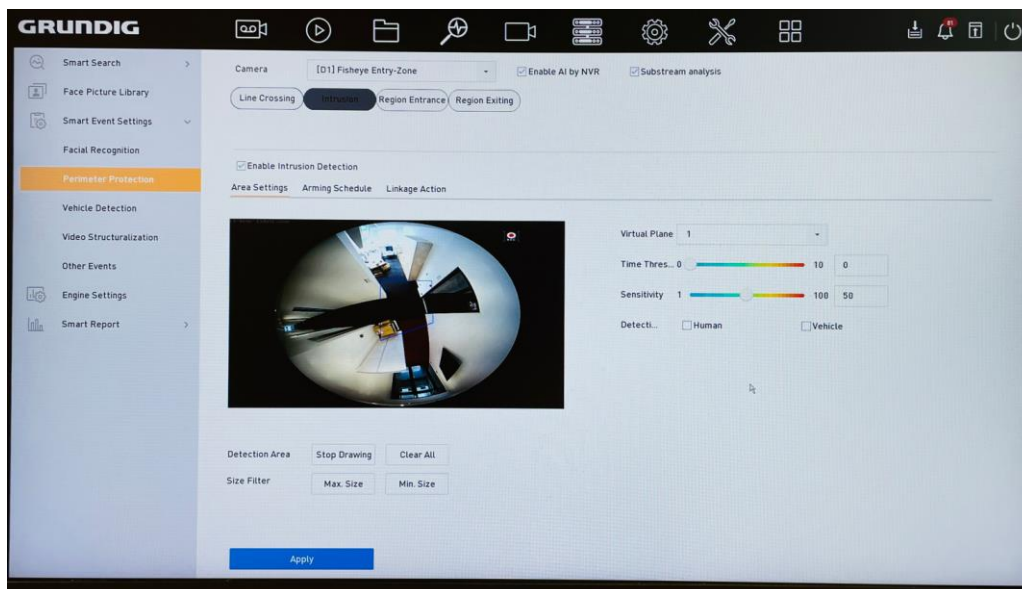



Figure 13-2 Intrusion Detection

6. Click **Rule Settings** to detection rules.
 - 1) Select a rule number. For example, select **1**.
 - 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set **Time Threshold**, **Sensitivity**, and **Detection Target**.

Time Threshold



The time an object loiters in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

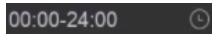
The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) Optional: Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
 - 5) Optional: Repeat above steps to draw more rules. Up to 4 rules are supports.
7. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

8. Click **Linkage Method** to set linkage methods.

Table 13-4 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record

Linkage Method	Description
	<p>videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

Please go to **System** → **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection** to enable **Perimeter Protection** algorithm.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. Optional: Turn on **Enable AI by NVR**.
The device will analyze the video, and cameras only transmit video stream.
4. Select **Region Entrance**.
5. Turn on **Enable**.

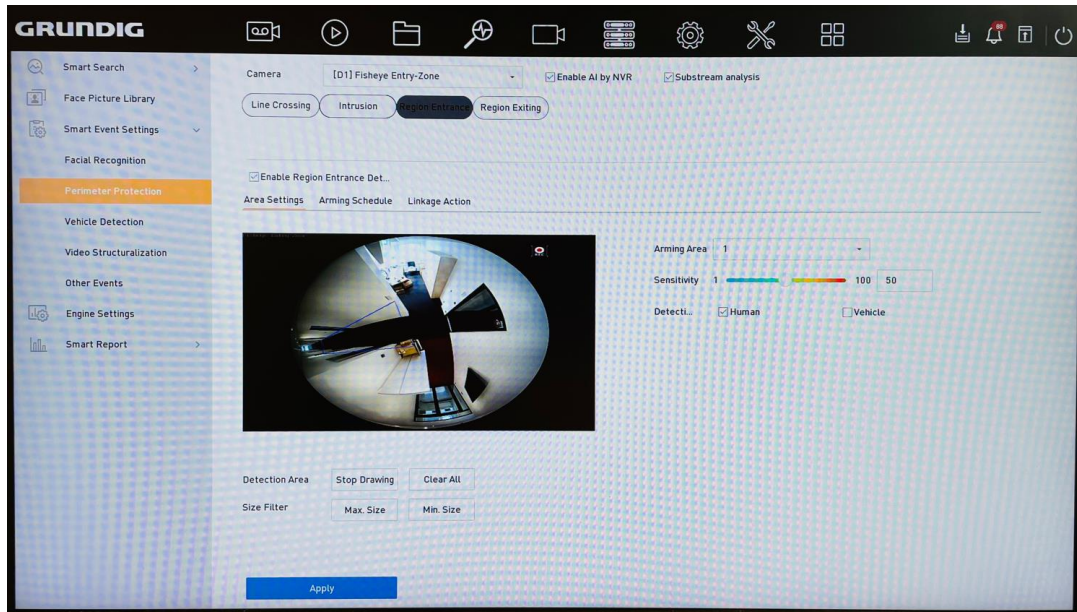



Figure 13-3 Region Entrance Detection

6. Click **Rule Settings** to detection rules.
 - 1) Select a rule number. For example, select **1**.
 - 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.


Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) Optional: Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

8. Click **Linkage Method** to set linkage methods.

Table 13-5 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.

Linkage Method	Description
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

Please go to **System** → **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection** to enable **Perimeter Protection** algorithm.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.

2. Select a camera.
3. Optional: Turn on **Enable AI by NVR**.
The device will analyze the video, and cameras only transmit video stream.
4. Select **Region Exiting**.
5. Turn on **Enable**.

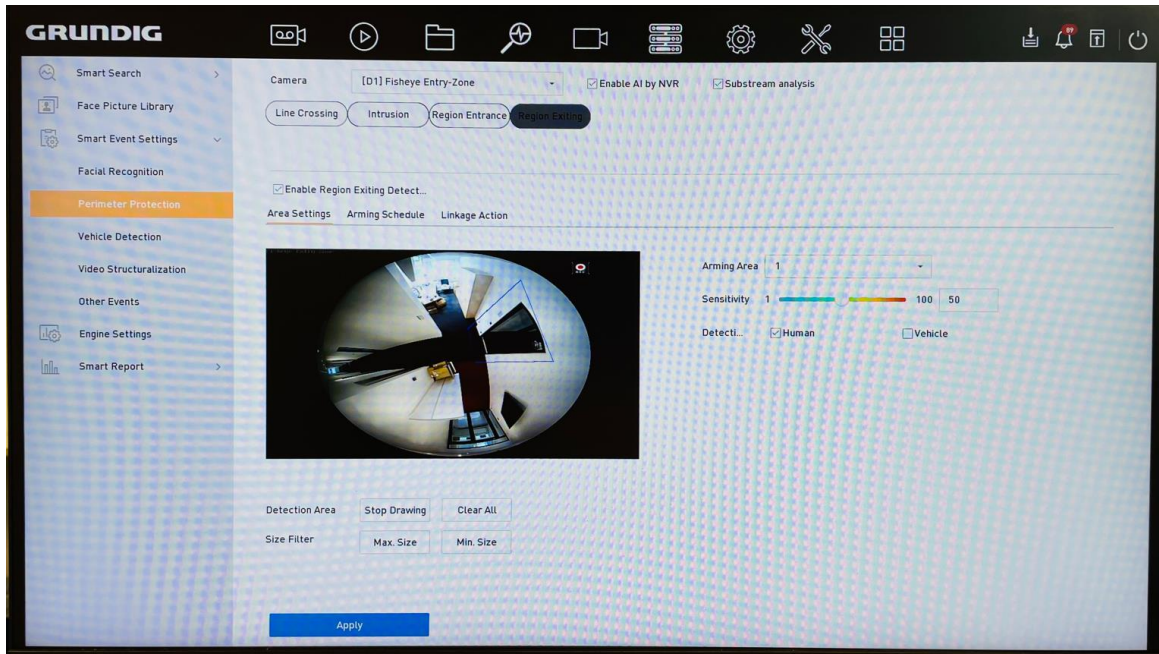



Figure 13-4 Region Exiting Detection

6. Click **Rule Settings** to detection rules.
 - 1) Select a rule number. For example, select **1**.
 - 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.


Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) Optional: Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

8. Click **Linkage Method** to set linkage methods.

Table 13-6 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Event**.
2. Select a camera
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

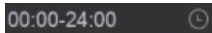
Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	<ol style="list-style-type: none"> 1. Select a rule number. 2. Use the tool bar at the top of image to draw the detection line. 4. Set Time Threshold and Sensitivity. <p>Time Threshold The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].</p> <p>Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.</p> 4. Optional: Repeat the above steps to set another one.
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	

<p>Object Removal Detection</p>	<p>The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.</p>	
<p>Fast Moving Detection</p>	<p>Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.</p>	
<p>People Gathering Detection</p>	<p>People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.</p>	<ol style="list-style-type: none"> 1. Select a rule number. 2. Use the tool bar at the top of image to draw the detection line. 3. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. 4. Optional: Repeat the above steps to set another one.

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>


8. Click **Save**.

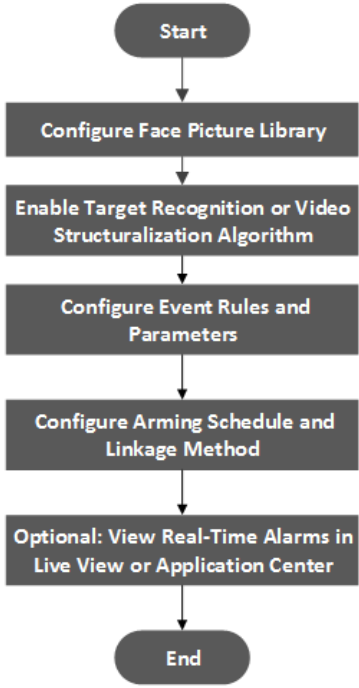
13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management**.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Target Event**.
2. Select a camera.
3. Select an event.
4. Turn on **Enable**.
5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can be triggered when a human face is detected.	-
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	 <pre> graph TD Start([Start]) --> Step1[Configure Face Picture Library] Step1 --> Step2[Enable Target Recognition or Video Structuralization Algorithm] Step2 --> Step3[Configure Event Rules and Parameters] Step3 --> Step4[Configure Arming Schedule and Linkage Method] Step4 --> Step5[Optional: View Real-Time Alarms in Live View or Application Center] Step5 --> End([End]) </pre> <p>Figure 13-5 Flow Diagram of Face Picture Comparison</p>

Target Grading

Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.

Non-Real-Time Mode

For places with a high flow of people, the device processing speed may not be fast enough, **Non-Real-Time Mode** will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. **Non-Real-Time Mode** will not trigger real-time alarm, so **Arming Schedule** is unavailable.

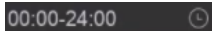
Linkage Succeeded / Linkage Failed

When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in **Target of Live View**.

Multi-Target-Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-
-----------------------------	--	---

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

8. Click **Save**.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

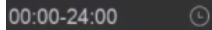
1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events**.
2. Select a camera.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-11 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or


Linkage Method	Description
	users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

8. Click **Save**.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to **Event Center** →  → **Normal Event** → **Alarm Input**.
2. Select an alarm input name.

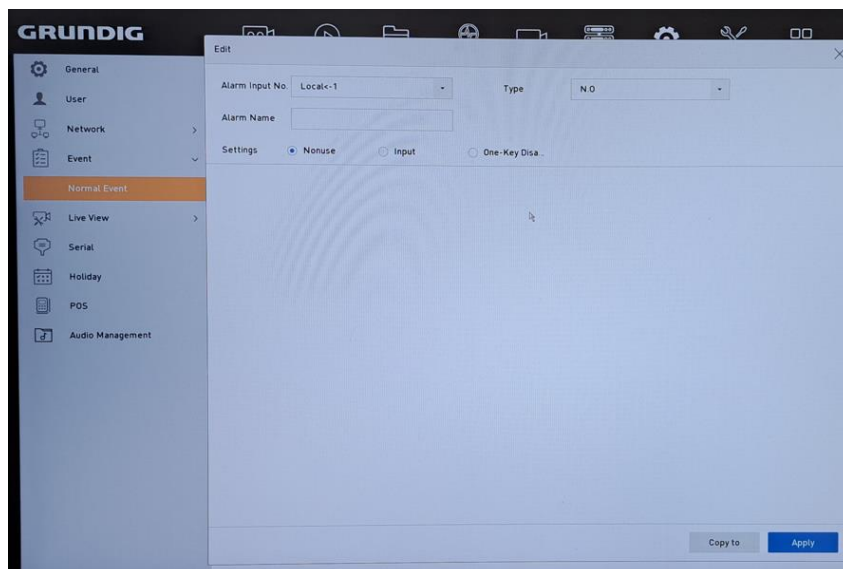


Figure 13-6 Configure Alarm Input

Note

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

3. Edit **Alarm Name**.
4. Turn on **Enable**.
5. Set **Quick Disarming**. Quick disarming can disable the selected alarm linkage methods in a batch.
6. Set **Alarm Type**.

Note

Refer to the alarm source to correctly configure the alarm type.

N.O


When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

8. Click **Linkage Method** to set linkage methods.

Table 13-12 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

9. Click **Save**.

13.1.7 Audio Analysis Event

Steps

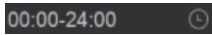
1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events**.
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-13 Audio Analysis Event

Event Name	Event Description	Rule Configuration
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	<p>Sudden Increase of Sound Intensity Detection Detects a steep sound increase in the scene.</p> <p>Sudden Decrease of Sound Intensity Detection Detects a steep sound drop in the scene.</p> <p>Sensitivity The higher the value is, the easier the detection alarm can be triggered.</p> <p>Sound Intensity Threshold It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.</p>

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-14 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.
Record	<p>When an alarm is detected, the selected channel would record videos.</p> <hr/> <p>Note</p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.</p> <hr/>

8. Click **Save**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

1. Go to **Event Center** →  → **Linkage Configuration**.
2. Click **Email** to configure email parameters.

Table 13-15 Email Linkage

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click **Audio Management** to manage audio files for alert linkage.

Note

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. Click **Alarm Output** to set alarm output parameters.

Note

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, **Local->1** means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

5. Click **Alarm Host** to set security control panel parameters.
6. Click **Flashing Light Alarm Output** to set the camera flashing light.
7. Click **Audio Alarm Output** to set the camera speaker.

13.3 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

1. Go to **Event Center** → .

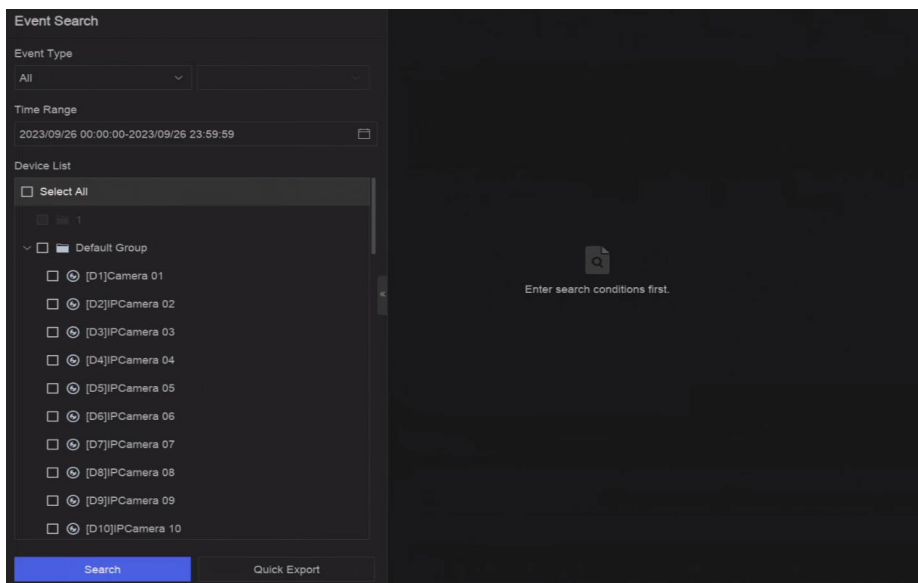


Figure 13-7 Event Search

2. Specify detailed conditions, including event type, time, channel, etc.
3. Click **Search**.
The device will display the searching results of the selected channel(s).


What to do next

Select the items from the result list and export them for backup.

13.4 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

1. Go to **Event Center** → .
2. Click **Real-Time Alarm**.
3. Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

4. Click **Playback**, and the alarm recording video would be played back.
5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to **Backup**.

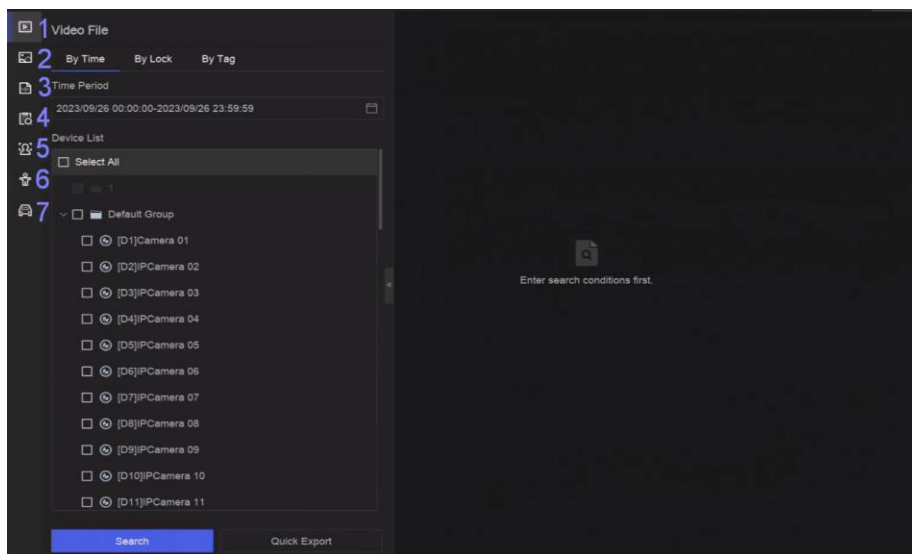


Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, several types are supported.

Note

The searching conditions would vary according to the selected searching method.

3. Set the searching conditions.
4. Click **Search**.



Figure 14-2 Searching Result

5. Optional: Perform the following operations.

- 1 Click to select a file.
- 2 Click to lock a file. After a file is locked, it will not be overwritten.
- 3 Click to export a file.
- 4 Use the tool bar at the top to filter results by channel.
- 5 Use the tool bar at the top to switch display effect.
- 6 Go to different result pages.
- 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.

6. Insert a USB flash drive to the device for backup.

7. Export files to the USB flash drive.

- Select file(s) in the result list and click **Export**.
- Click **Export All** to export all the files.

15 Smart Settings

15.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to **Smart Analysis** → **Engine Settings**. The available algorithms would be listed, and you can click the required algorithm to link engine(s).

15.2 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers'** library is used to store pictures for strangers, and it cannot be deleted.

15.2.1 Add a List Library

Steps

1. Go to **Smart Analysis** → **Face picture Library**.
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.

Note

- After a list library, you can move the cursor on the library to edit or delete it.
 - You can click **Delete in Batch** to delete selected libraries, or clear all pictures in the selected libraries.
-

15.2.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start


- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

1. Double click a list library.
2. Optional: Click **Custom Tag** to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.

3. Click **Add** or **Import**.

4. Import picture(s).

- **Add:** Click  to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
- **Import:** Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.

5. Optional: Perform the following operations.

- Delete Pictures from the Library**
- Select a picture and delete it.
 - Select pictures and click **Delete in Batch** to delete the select ones.

Search Pictures in the Library Click  at the tool bar to search pictures.

Copy Pictures to Another Library Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.

Edit Pictures Click the picture name, and edit its attributes.

Export Pictures Select pictures, and click **Export** to export them to a USB flash drive.

16 Application Center

16.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time. Human and vehicle detection should be configured in advance. Go to **System** → **Event** to configure.



Figure 16-1 Human and Vehicle Detection

Table 16-1 Human and Vehicle Detection Description

No.	Description
1	Right-click to display menu bar.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

16.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

16.2.1 Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to **Smart Analysis** → **Smart Event Settings** → **Face Recognition**. Allocate **Target Recognition** to at least one engine.
- The list library for check-in comparison is properly configured. Refer to **Add a List Library** for details.

Steps

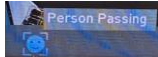
1. Click **Person Passing** .
2. Click **Search Record**.
4. Choose camera and time range and click **Search**.



Figure 16-2 Check-In Task


16.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to **Person Check-In**.
2. Right click to display the menu at the left side.
3. Click .

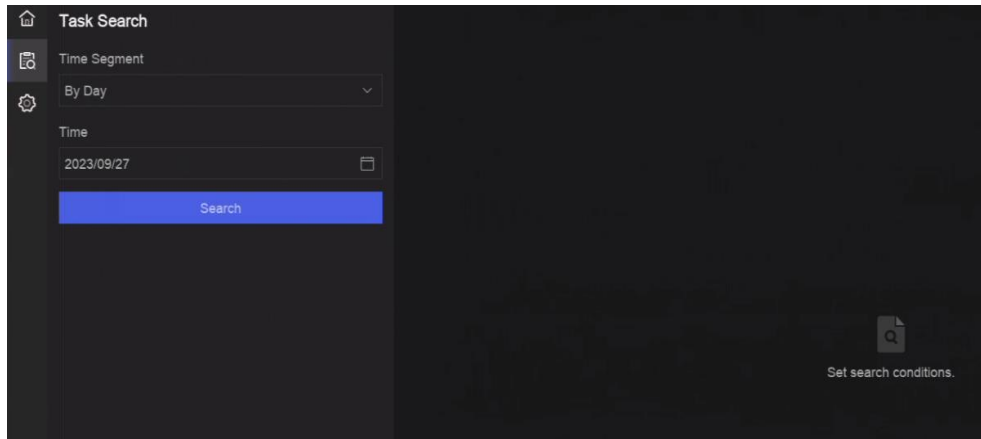




Figure 16-3 Search Check-In Records

4. Set time.
5. Click **Search**.

16.3 Statistic Report

You can view reports of people counting and heat map.

Table 17-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		<ul style="list-style-type: none"> ● The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. ● Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.
Heat Map		<ul style="list-style-type: none"> ● The function must be supported by the connected IP camera. ● Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

17 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.
Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Table 17-1 Parameter Description

Type	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time Configuration	Time Sync Mode	NTP Time Sync Your device can connect to a network time protocol server to ensure that the system time is accurate. Manual Time Sync. Manually set the system time.
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console After connecting it to PC with a convertor, PC can set the device parameters. Transparent Channel It is directly connected to a serial device. PC can remotely access the serial device through network.

18 Hot Spare Device Backup

The video recorder GD-RN-DT8864N can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.

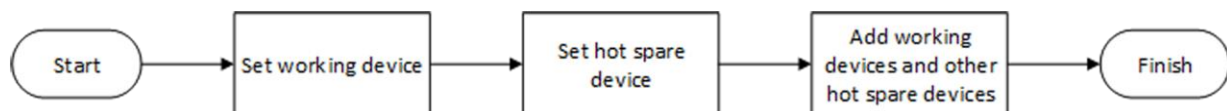


Figure 18-1 Build a Hot Spare System

Note

- Up to 32 working devices and 32 hot spare devices are allowed.
 - It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
-

18.1 Set Working Device

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare**.
2. Set **Working Mode** as **Normal Mode**.
3. Turn on **Enable**.
4. Click **Save**.
5. Optional: View **Hot Spare Device IP Address** and **Hot Spare Device Working Status**.

18.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare**.
2. Set **Working Mode** as **Hot Spare Mode**.
3. Click **Save**. Your device will restart automatically.

Note

- The camera connection will be disabled when the device works in hot spare mode.
 - It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.
-

4. Go to **System** → **System Management** → **N+M Hot Spare** again.
5. Add working devices to the hot spare system.
6. Add hot spare devices to the hot spare system.
7. Click **Save**.

19 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System** → **Event** → **Exception**.

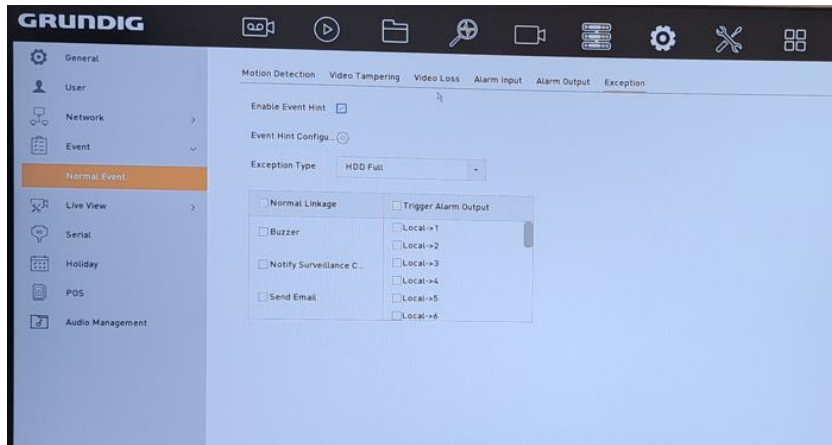




Figure 19-1 Exception Event Configuration

2. Select exception type.
3. Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software SCMS.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any other events.

Note

When exception events occur,  at the upper-right corner would notify, and you can click  to view.

4. Click **Save**.

20 View System Info

Go to **Maintenance** → **System Info** → **Device Info** to view the system information.



Figure 20-1 System Info

21 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

21.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to **System** → **System Maintenance** → **Maintenance** → **Schedule Reboot** to enable the function, and set the reboot schedule.

21.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** → **System Maintenance** → **Maintenance** → **Upgrade** to upgrade your device.

21.3 Backup and Restore

Go to **System** → **System Maintenance** → **Maintenance** → **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

The device configuration files can be exported to a local device for backup, and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Simple Restore

Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the device to the inactive status, and leave all settings unchanged except restoring user accounts.

21.4 Log Info

Go to **System** → **System Maintenance** → **Maintenance** → **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

21.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

1. Go to **System** → **CX** → **System Settings** → **Network** → **Network** → **Log Server**.
2. Turn on **Enable**.
3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. Optional: Click **Test** to test if parameters are valid.
5. Click **Save**.

21.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

1. Go to **System** → **System Maintenance** → **Maintenance** → **Maintenance Tools**.
2. Select tools according to your requirement.

Table 21-1 Tool Description

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	

HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replace the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.

Note

It is recommended to use maintenance tools with the help of technical support.

22 Security Management

22.1 Address Filter

22.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

1. Go to **System** → **System Maintenance** → **Security Management** → **Stream Encryption**.
2. Turn on **Enable**.
3. Set **Encryption Key**.

Note

The stream encryption key is synchronized with the SCMS service verification code. After enabling the encryption code, the SCMS stream will be forcedly encrypted.

4. Click **Save**.

22.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to **System** → **System Maintenance** → **Security Management** → **TLS** to select TLS version.

23 Appendix

23.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, $\Phi 2.1$	Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	Channel Well Technology Co., Ltd.

23.2 Glossary

Dual-Stream

Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

DDNS

Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

Acronym for National Television System Committee. NTSC is an analog television standard used

in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

NVR

Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

23.3 Frequently Asked Questions

23.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera** → **Video Parameters** → **Sub-Stream**. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

Note

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

2433.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

23.3.3 Why is the video recorder notifying the stream type is not supported?**Reason**

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

23.3.4 How to confirm the video recorder is using H.265 to record video?**Solution**

Check if the encoding type at live view toolbar is H.265.

23.3.5 Why is the video recorder notifying IP conflict?**Reason**

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

23.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?**Reason**

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on another device, change your HDD, and try again.

23.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTV, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

23.3.8 Why does the PTZ seem unresponsive via RS-485?**Reason**

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

23.3.9 Why is the video sound quality not good?**Reason**

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.

23.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the

requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Table 24-1 Corrosive Gas Concentration Limit

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCl (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _x (Nitrogen Oxides)	0.5	1.0

Note

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Table 23-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _x (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.

Category	Primary Sources
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.

